Training Navy Employees to Protect Data at Home and on the Road

By Lt. Sean W. Kelley

Background

Department of Navy (DON) employees frequently work at home. In the office, there is a staff dedicated to the protection of data. But how safe are data when employees work at home or on the road?

The Gartner Group estimated that by 2008, 41 million corporate employees globally will spend at least one day a week teleworking, and 100 million will work from home at least one day a month. The highest proportion of these will be U.S. workers. Further, Gartner specifies that these numbers do not represent the number of employees that are on the road for official business.

In addition, findings from the Gartner Symposium/ITxpo 2003, reported that wireless users in North America will grow from 4.2 million in 2003 to more than 31 million in 2007.

Working at home is an opportunity for personnel to spend time with their families while preparing for the next day, and many of us are often required to work in a mobile environment. But these statistics should make the need for a home security training program even more obvious.

It is crucial for all organizations to look at home network use when building their data security strategy. Every organization should have an Information Security Awareness Program. Each ISAP should cover the requirements of Navy information assurance. The goal of IA is to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. Information assurance is essential for warfighting and homeland defense, and is required operationally throughout the Department.

Mandatory Training

All authorized users (military, civilians and contractors) of Department of Defense information systems were required to complete IA awareness orientation training by Sept. 1, 2005. IA awareness training is available for the DON through Navy Knowledge Online (http://www.nko.navy.mil) and MarineNet (http://www.marinenet.usmc.mil).

Depending on your organization, the command information assurance manager (IAM), information assurance officer (IAO) or information systems security manager (ISSM) is responsible for ensuring that all personnel with active user accounts complete initial or refresher training.

The course takes about 30 minutes to complete and explains the importance of classified information and how to protect it from unauthorized users both inside and outside the workplace.

For more information and step-by-step instructions for accessing IA training, please visit the IA workforce page of the DON Chief Information Officer (CIO) Web site at http://www.doncio.navy.mil/iaworkforce/.

The DON has deployed this centralized training module, but training should be complemented with a comprehensive training program at each command to include the protection of unclassified data and networks.

Training should include the security requirements of what to do when working at home and on the road. For guidance, refer to the Secretary of the Navy Information Assurance Manual (SECNAV M-5239.1) of November 2005 (http://neds.daps.dla.mil/Directives/5239_1.pdf/).

DON Guidance

The Bureau of Naval Personnel Instruction 12300.2 defines the requirements of the Navy's Telecommuting (Telework) Program. The instruction states: "At a minimum, all telework agreements must address the location and requirements of the alternative worksite, telework schedule, security of official information, protection of Government-furnished equipment, applicable standards of conduct, liability and injury compensation, and Government access to the alternative work site."

Per the DoD Telework Policy (Oct. 2002), the primary medium for teleworking on a regular basis *(one day or more per pay period)* should be a government-provided desktop or laptop computer or BlackBerry device. Personal computers may be used for ad hoc teleworking on limited amounts of sensitive unclassified material, as long as it is deleted once no longer required.

Ad hoc access to DON e-mail or scheduling functions through Outlook Web Access, requires command approval for access to OWA, a computer meeting the required configuration, and the use of a Public Key Infrastructure (PKI) certificate for authentication.

Users will need a Common Access Card (CAC) reader and the associated middleware on their personal computer to enable PKI authentication. The current DON policy, including computer configuration requirements, is available by searching for "remote access" on the DON CIO Web site at http://www.doncio.navy.mil/.

DON organizations should take steps to ensure that teleworkers and travelers are properly trained. In some cases, I have seen users connect to hotel networks and accidentally load malicious software on their personal laptop or computer resulting in the inability to complete their work. How does the DON deal with these issues?

Free Antivirus Protection

Antivirus software that provides multilayered protection at the desktop, server, gateway and network levels is available for download at no charge to your organization. Antivirus software available for download includes McAfee, Symantec and Trend Micro products.

DoD users with a dot-mil address, including all combatant commands, military services, agencies and military academies; personnel within joint, NATO and coalition forces; contractors authorized to use government-furnished equipment; and the Coast Guard are authorized to download and use this software.

Products are available for home computers, home and office firewalls, and wireless or personal digital assistants. By expanding products to home use, the DoD is acknowledging that safeguarding computers at home is as important as safeguarding computers in the workplace. These products can be downloaded by linking to either of the following Web sites.

NIPRNET Site: http://www.cert.mil/antivirus/av_info.htm

SIPRNET Site: http://www.cert.smil.mil/antivirus/av_info.htm

Build a Defensive Program

For teaching a home security course, allow at least three hours for instructor-led training. Tailor the presentation to home and mobile users. Try to brief to the lowest knowledge level but ensure the advanced user is also challenged.

Below is a sample outline identifying material that should be covered.

√ Explain the importance of computer security and how it should be applied to home use.

√ Provide statistics regarding Internet threats. For example, Carnegie Mellon's CERT® Coordination Center Web site maintains incidents up to 2003. Though it discusses corporate statistics, it illustrates how Internet threats have grown: 1998 – 6 incidents; 2003 – 137,529 incidents.

√ Explain the consequences of malicious code: viruses, worms, Trojans and spyware, and the dangers of opening e-mail attachments from unknown sources.

√ Explain the importance of backing up data!

√ Discuss the importance of having an antivirus, firewall and spyware removal tool on home and laptop computers and keeping them up to date.

√ Explain the dangers of broadband access, wireless networks and security.

√ Explain what to do if computing devices have been hacked or there is a security violation.

√ Discuss phishing scams and spoofed e-mails.

√ Direct the use of good password management using strong passwords that are changed every 90 days.

For home users discuss identity theft and scams, Web browser security and protecting children from the dangers of chatrooms, blogs, pornography and "MySpace." Discuss Web protection and Web filtering mechanisms and online music downloads and software piracy.

Discuss environmental controls, such as electric power and uninterruptible power supply, temperature, humidity and the consequences of spilling food or drinks on computing equipment.

I advocate a classroom setting, but if that is not feasible, online training is the next best option, but ensure that there is a mechanism to encourage user discussion and to answer questions.

Be Vigilant!

Thanks to the Internet we can stay connected at home, on the road and in the office. But the data DON personnel handle in mobile settings are as important as data handling in the office.

Use of antivirus software with current virus definitions, a personal firewall, antispyware software, and PKI are all tools that can help ensure safe and secure computing from both home and mobile environments. A virus that destroys your files at home results in lost productivity and may be a source of vulnerability to Navy networks.

Telework will change the lifestyles of DON users to enable a more flexible work environment, but users must remain vigilant in protecting data. Our lives could depend on it!

Resources

In addition to DON and DoD guidance organizations like Carnegie Mellon's CERT® Coordination Center and the SANS Institute have created home network security education guidance. Microsoft has a Web site devoted to educating the home user on security matters at http://www.microsoft.com/athome/security/default.mspx/.

The SANS Institute offers a "Computer and Network Security Awareness" course that can be purchased for $1,000 for a one-year subscription. Purchasers can make unlimited copies for their organizations for the subscription period. More information is available at http://www.sans.org/staysharp/description.php?tid=311/.

Additional resources to assist you in building your home security awareness course are available at the CERT Coordination Center's Home Network Security Web site at http://www.cert.org/tech_tips/home_networks.html.

The National Cyber Alert System was created by US-CERT and the Department of Homeland Security to help you protect your computer. One of US-CERT's overarching goals is to ensure that you have access to timely information about security topics and events. Go to http://www.us-cert.gov/referral_pg/.

Home PC Firewall Guide: http://www.firewallguide.com/.

ProtectKids.com: http://www.protectkids.com/dangers/.

"Cyberwatch" - a cyber safety site by M.E. Kabay Ph.D., associate professor of information assurance at Norwich University: http://www2.norwich.edu/mkabay/cyberwatch/index.htm.

Lt. Sean W. Kelley is the head for Information Technology and Communication Services at the Bureau of Medicine and Surgery. He is a Medical Service Corps officer with an IM/IT subspecialty. He has a master's degree in computer resource and information management from Webster University and a master's degree in information systems technology from the Naval Postgraduate School. CHIPS